Preface to the special issue on Formal Methods for Industrial Critical Systems (FMICS 2007 + FMICS 2008).

Science of Computer Programming 76 (2011) 63–64

Contents lists available at ScienceDirect

Science of Computer Programming

journal homepage: www.elsevier.com/locate/scico

Editorial

Preface to the special issue on Formal Methods for Industrial Critical Systems (FMICS 2007 + FMICS 2008)

1. Introduction

This special issue contains improved versions of selected papers from the workshops on Formal Methods for Industrial Critical Systems (FMICS) held in Berlin, in July 2007 and in L'Aquila, in September 2008. These were, respectively, the 12th and 13th of a series of international workshops organized by an open working group supported by ERCIM (European Research Consortium for Informatics and Mathematics) that promotes research in all aspects of formal methods (see details in http://www.inrialpes.fr/vasy/fmics/). The FMICS workshops that have produced this special issue considered papers dealing with the following themes:

- Design, specification, code generation and testing with formal methods.
- Verification and validation of complex, distributed, real-time systems and embedded systems.
- Verification and validation methods that aim at circumventing the shortcomings of the existing methods with respect to their industrial applicability.
- Tools for the design and development of formal descriptions.
- Case studies and project reports on formal methods related projects with industrial participation (e.g. safety critical systems, mobile systems, object-based distributed systems).
- Impact of the adoption of formal methods on the development process and associated tools.
- Application of formal methods in standardization and industrial forums.

The selected papers are the result of several evaluation steps. Initially, FMICS 2007 received 31 papers and FMICS 2008 received 36 papers, with 15 and 14 accepted, respectively. After the workshops, selected papers were published in Lecture Notes in Computer Science (volumes 4916 [1] and 5596 [2]). Then, the authors of 6 papers were invited to submit extended journal versions to this special issue. Most of these papers passed two review phases, and finally 5 were accepted to be included in the journal.

2. Selected papers

The whole selection process was open to the themes of the workshops; however the final list of papers has a common focus on the automatic verification of systems. This witnesses the current concerns about the importance of automatic verification, which is on the one hand gaining more and more industrial application, especially in the field of interest of FMICS, that is, critical systems: model checking and static analysis techniques are routinely applied in several industrial domains. On the other hand, application to real systems often stresses such verification techniques to their limits, requiring new insights and techniques for helping scalability of automatic verification to the size of the increasingly complex systems that more and more pervade our daily lives. The collection of papers gathered in this special issue is a good representative of the research carried out in this direction.

The first paper by Guodong Li, Robert Palmer, Michael DeLisi, Ganesh Gopalakrishnan and Robert M. Kirby considers how to deal with Application Programming Interfaces (API) when making formal models of software. In particular, the authors develop a formal model of the Message Passing Interface (MPI), which is widely used for High Performance Computing. This formalization can help avoid misunderstandings; however its most interesting use is to support the automatic verification of C code that uses MPI.

In the second paper, Bernard van Gastel, Leonard Lensink, Sjaak Smetsers and Marko van Eekelen present verification work on one industrial implementation of the reentrant readers–writers problem. They use the model checker SPIN to check deadlock for a fixed configuration and the theorem prover PVS to extend the analysis to any number of processes.

0167-6423/$ – see front matter
doi:10.1016/j.scico.2010.07.001

The paper by Bastian Schlich, Jörg Brauer and Stefan Kowalewski provides real applications of static analysis to reduce the resources needed to perform model checking. In particular, they apply dead variable reduction and path reduction to a microcontroller binary code. They present the new model checker [MC]SQUARE and its application to several microcontroller codes.

Maurice H. ter Beek, Alessandro Fantechi, Stefania Gnesi and Franco Mazzanti deal with the problem of verifying concurrent systems specified with UML state machines. Their approach consists in defining different levels of abstraction at which one wants to reason in order to control the amount of information needed in the verification. They develop a new verification framework for UML and present an application to the UML framework, based on a case study coming from an automotive scenario studied in the Service Oriented Computing domain.

Finally, in the fifth paper, Stefan Edelkamp, Damian Sulewski, Jiri Barnat, Lubos Brim and Pavel Šimeček discuss the use of flash memory to store the state for on-the-fly and off-line model checking. They propose optimized algorithms considering the access to this kind of memory. The paper focusses on new approaches to hashing supported by experimental evaluation.

Acknowledgements

We would like to thank all the authors, the members of the program committees and the reviewers of the two workshops, and the reviewers of the journal versions for their efforts in preparing and reviewing papers. We also especially thank Bas vas Vlijmen, Gerard Berry and Saveetha Balasundaram for their valuable support in the whole revision and editing process.

References

[1] S. Leue, P. Merino (Eds.), Formal Methods for Industrial Critical Systems (12th International Workshop, FMICS 2007, Berlin, Germany, July 1–2, 2007, Revised Selected Papers), in: Lecture Notes in Computer Science, vol. 4916, Springer, 2008.
[2] D.D. Cofer, A. Fantechi (Eds.), Formal Methods for Industrial Critical Systems (13th International Workshop, FMICS 2008, L'Aquila, Italy, September 15–16, 2008, Revised Selected Papers), in: Lecture Notes in Computer Science, vol. 5596, Springer, 2009.

Darren Cofer
Rockwell Collins, USA
E-mail address: ddcofer@rockwellcollins.com.

Alessandro Fantechi
University of Florence, Italy
E-mail address: fantechi@dsi.unifi.it.

Stefan Leue
University of Kostanz, Germany
E-mail address: Stefan.Leue@uni-konstanz.de.

Pedro Merino*
University of Malaga, Spain
E-mail address: pedro@lcc.uma.es.

Available online 30 July 2010

* Corresponding editor.